UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/574,808	01/30/2007	David Jeal	P08887US00/RFH	1885

881 7590 02/23/2010

STITES & HARBISON PLLC
1199 NORTH FAIRFAX STREET
SUITE 900
ALEXANDRIA, VA 22314

EXAMINER	
RAVETTI, DANTE	
ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
02/23/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/574,808	JEAL ET AL.	
	Examiner	Art Unit	
	DANTE RAVETTI	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-129* is/are pending in the application.

4a) Of the above claim(s) *See Continuation Sheet* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *See Continuation Sheet* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Disposition of Claims: Claims withdrawn from consideration are 3,4,8-10,13-16,18,21,24,26,28,29,35,40-51,54,55,59,60,62-65,67,70,73,77,78,84 and 89-129.

Continuation of Disposition of Claims: Claims rejected are 1,2,5-7,11,12,17,19,20,22,23,25,27,30-34,36-39,52,53,56-58,61,66,68,69,71,72,74,76,79-83 and 85-88.

DETAILED ACTION

Acknowledgements

1. This communication is in response to the amended Application No. 10/574,808 filed on December, 14, 2004.

2. Claims 101-129 have been withdrawn by the Applicant.

3. Claims 3-4, 8-10, 13-16, 18, 21, 24, 26, 28-29, 35, 40-51, 54-55, 59-60, 62-65, 67, 70, 73, 77-78, 84, 89-100 have been cancelled by the Applicant.

4. Claims 1-2, 5-7, 11-12, 17, 19-20, 22-23, 25, 27, 30-34, 36-39, 52-53, 56-58, 61, 66, 68-69, 71-72, 74, 76, 79-83, 85-88 are currently pending and have been fully examined.

5. For the purpose of applying the prior art, PreGrant Publications will be referred to using a four digit number within square brackets, e.g. [0001].

Response to Applicant's Remarks/Amendments

6. Applicant's response filed November 4, 2009 has been fully considered, but are not persuasive. Applicant argues:

> The present invention teaches the possibility of authenticating a transaction using predetermined authentication information stored on an authentication storage means. Crucially, the user authentication means need not be inserted into a user device. Rather, the authentication storage means (e.g., a SIM) need only be coupled to a device for reading the authentication storage means to obtain the authentication information when that is needed to authenticate the transaction.
>
> Malinen fails to teach the possibility of dissociating the authentication storage means from a user terminal. This is consistent with the industry prejudice at the time of filing: SIM cards were assumed to be integral with a given user device (mobile nodes) for the purpose of authenticating transactions.

However, Applicant's Specification recites:

> [0045] In a more specific example, **the smart card is a Subscriber Identity Module or SIM of the type used in and for authenticating the use of handsets in a mobile or cellular telecommunications network--such as a GSM (Group Special Mobile) or 3G (Third Generation) network**. Such a network will store details of its users' (subscribers') SIMs. In operation of the network, a user's handset is authenticated (for example, when the user activates the handset on the network with a view to making or receiving calls) by the network sending a challenge to the handset incorporating that SIM, in response to which the SIM calculates a reply (dependent on the predetermined information held on the SIM--typically an authentication algorithm and a unique key Ki) and transmits it back to the network which checks it against its own information for that user or subscriber in order to complete the authentication process. In the same way, therefore, the SIM can be used in or in association with the data processing apparatus or computer so that the same form of authentication process can be carried out. In a case where the SIM is the SIM of a subscriber to a particular cellular telecommunications network, the authentication process can be carried out by that network.
>
> [0047] **The SIM need not take the form of a physical (and removable) smart card but instead can be simulated by being embedded in the data processing apparatus or computer in the form of software** or represented as a chip for example.
>
> [0064] **In an alternative arrangement, a data carrier may be provided with means for storing predetermined information such as in one of the forms described above--that is, a SIM or (more probably) software simulating a SIM**. The simulated SIM is associated with data stored on the data carrier. The data carrier may, for example, be a DVD or CD ROM or some other similar data carrier, and the data thereon may be software or a suite of software.

However, the cited prior art of *Malinen* expressly teaches:

> [0024] The three party trust model described herein may also allow an entity, such as a financial institution or a network operator, an opportunity to authorize specific services. Such an entity might have, for example, a well-developed authorization infrastructure, **e.g., by using widely distributed smart cards.** The three party trust model may be used to allow a provider of services to grant a service without using its own authorization infrastructure.

Therefore, the cited prior art of *Malinen* expressly teaches the distribution of "smart cards" (e.g. SIM cards) as part of an authorization infrastructure.[1]

In light of Applicant's choice to pursue method claims, Applicants are also reminded that functional recitations using the word "for," "configured to," or **other functional terms** (e.g. see claim 1, which recites, "providing a data processing apparatus, in which the entity generates....") have been considered but are not given

patentable weight[2] because they fail to add any structural limitations and are thereby regarded as intended use language. To be especially clear, all limitations have been considered; however, a recitation of the intended use in a product claim must result in a structural difference between the claimed product and the prior art in order to patentably distinguish the claimed product from the prior art. If the prior art structure is capable of performing the intended use, then it reads on the claimed limitation.[3]

Claim 7 contains similar language as found in claim 1.

Examiner would like to point out that the language of claim 1, and in others, describes "descriptive" material and thereby does not receive patentable weight (e.g. "...the authentication storage means being registerable with a common....").

Claims 11, 20 contains similar language found in claim 1.

Examiner would like to point out that the language of claim 2, and in others, describes, "non-functional descriptive material." For example, as to claim 2, Applicant recites, "...the predetermined authentication information stored by each authentication storage means corresponds to information which is used to authenticate a user of that authentication storage means in relation to the system ..." However, this is an example of non-functional descriptive material.[4]

---

[1] In re Lindberg, 93 USPQ 23 (CCPA 1952); It is not regarded as inventive to merely make an old device portable or movable without producing any new and unexpected result;
[2] In re Gulack, 703 F. 2d 1381, 217 USPQ 401, 404 (Fed. Cir. 1983)(stating that although all limitations must be considered, not all limitations are entitled to patentable weight);
[3] In re Casey, 370 F.2d 576, 152 USPQ 235 (CCPA 1967) ("The manner or method in which such machine is to be utilized is not germane to the issue of patentability of the machine itself."); In re Otto, 136 USPQ 458, 459 (CCPA 1963). See also MPEP §§ 2114 and 2115. Unless expressly noted otherwise by the Examiner, the claim interpretation principles in this paragraph apply to all examined claims currently pending.
[4] Wherein --MPEP 2114; In re Swineheart, 169 USPQ 226; In re Schreiber, 44 USPQ2d 1429 (Fed. Cir. 1997); While features of an apparatus may be recited either structurally or functionally, claims directed to an apparatus must be distinguished from the prior art in terms of structure rather than function alone.

Examiner would also like to point out that Official Notice was used in the previous office action mailed on 4 May 2009 to indicate that *incorporating an authentication storage means on a data carrier is old and well known in the art.* Since Applicant has not attempted to traverse this Official Notice statement, examiner is taking the common knowledge or well-known statement to be admitted prior art.[5]

As to claim 6, Applicant recites, "...transaction **when** the smart card or subscriber identity module is operable ...." The MPEP interprets claim limitations that contain "if, may, might, can, **when**, could and upon" statement(s), as optional language. As matter of linguistic precision, optional claim elements do not narrow claim limitations, since they can always be omitted.[6] Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation.

Therefore, after careful review of all of the Applicant's points of contentions, the Examiner respectfully disagrees and maintains his rejection.

Priority

7. Applicant's claim for the benefit of a prior-files application under 35 U.S.C. §119(e) or under 35 U.S.C. §120, §121, or §365(c) is acknowledged. Priority for this application is set to October 9, 2003, the filing date of the Foreign Application #: 0323693.2.

The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original non-provisional

[5] MPEP 2144.03 C;

application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficiently to comply with the requirements of the first paragraph of 35 U.S.C. §112.[7]

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. §112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1-2, 5-7, 11-12, 17, 19-20, 22-23, 25, 27, 30-34, 36-39 52-53, 56-58, 61, 66, 68-69, 71-72, 74, 76, 79-83, 85-88 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the authentication process" in claim 1. There is insufficient antecedent basis for this limitation in the claim. The process of "authentication" has not occurred prior to this limitation.

As to claim 1, Applicant recites, "...carrying out the authentication process via a communications link with that-the telecommunications .system, the authentication process being carried out by authenticating means incorporated in the telecommunications system **and involving the use of the transaction data** and the predetermined authentication...**transmitting, wherein in order to authenticate the transaction, the transaction data is transmitted between the data processing apparatus** and the telecommunications system via a transaction manager implemented by the data processing apparatus, and also transmitting the predetermined

[6] In re Johnston, 77 USPQ2d 1788 (Fed. Cir. 2006);

authentication information is also transmitted between the authentication storage means and the telecommunications .system via the transaction manager." Therefore, the scope of the claim is not clear, because the Applicant seems to be transmitting "transaction data" in order to authenticate, when the "transaction data" is already used by the authentication means to carry out the authentication. The appropriate correction is required.

Claim 1 is rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps.[8] The omitted steps are: the step of authenticating.

The term "predetermined" in claim 1 is a relative term which renders the claim indefinite. The term "predetermined" is not defined by the claim, the Specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The term "predetermined" in Applicant's Specification seems to be silent on who makes this "predetermination," what elements are used to derive this "predetermination," or when or how this "predetermination" is actually achieved. Just stating "predetermined," may not be sufficient.

Claims 12, 22, 52 and 71 contains similar language or like deficiencies found in claim 1.

As to claim 17, Applicant recites, "including operatively coupling the authentication storage means to a carrier." However, it is not clear what is actually

[7] See Transco Products, Inc. v. Performance Contracting, Inc., 38 F.3d 551,32 USPQ2d 1077 (Fed. Cir. 1994).
[8] MPEP § 2172.01

performing the coupling or how it is being accomplished; therefore, the scope of the claim is not clear.

As to claim 52, Applicant recites, "...with the data processing apparatus **not requiring use of that user's telecommunications terminal**." However, the scope of the claim is not clear. For example, does the Applicant infer that no information is received from the user's telecommunications terminal? The appropriate correction is required.

Claims 2, 5-7, 11-12, 17, 19-20, 22-23, 25, 27, 30-34, 36-39, 53, 56-58, 61, 66, 68-69, 71-72, 74, 76, 79-83, 85-88 are also rejected for being dependent upon rejected claim 1.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. §103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-2, 5-7, 11-12, 36-39, 52-53, 56-58, 61 and 85-88 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Malinen et al.*, (US 2003/0028763) ("*Malinen*").

As to claim 1:

Malinen teaches substantially as claimed:

> providing a data processing apparatus, in which the entity generates transaction data relating to the transaction (Abstract, [0005]-[0007], [0070]-[0074]), and

at least during the authentication process the data processing apparatus has operatively associated therewith a selected one of a plurality of authentication storage means respective to the users each for storing predetermined authentication information (Abstract, [0006], [0009], [0011], [0016], [0067]),

the authentication storage means being registerable with a telecommunications common system for which the users have respective telecommunications terminals ([0157], [0180]),

carrying out the authentication process via a communications link with the telecommunications system, the authentication process being carried out by authenticating means incorporated in the telecommunications system and involving the use of the transaction data and the predetermined authentication information stored by the selected one authentication storage means (Abstract, [0006], [0009], [0011], [0016], [0076], [0079], Figure 8-10),

transmitting in order to authenticate the transaction, the transaction data between the data processing apparatus and the telecommunication system via a transaction manager implemented by the data processing apparatus, and also transmitting the predetermined authentication information between the authentication storage means and the telecommunications system via the transaction manager (Abstract, [0006]-[0007], [0009], [0011], [0023], [0070]-[0074]).

Malinen does not expressly teach:

the predetermined authentication information stored by each authentication storage means corresponding to information which is used to authenticate a telecommunications terminal of that user in relation to the telecommunications system but the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of that user's telecommunications terminal;

However, Office Notice is taken that *predetermined authentication information stored by each authentication storage means corresponding to information which is used to authenticate a telecommunications terminal of that user in relation to the telecommunications system but the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of that*

user's telecommunications terminal. For example, in the related art of user authentication, it is common to employ the use of a portable authentication means. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of *Malinen* with the commonly recognized practice of *predetermined authentication information stored by each authentication storage means corresponding to information which is used to authenticate a telecommunications terminal of that user in relation to the telecommunications system but the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of that user's telecommunications terminal.*

As to claims 2 and 53:

Malinen expressly teaches:

> in which the predetermined authentication information stored by each authentication storage means corresponds to information which is used to authenticate a user of that authentication storage means in relation to the telecommunications system (Abstract, [0009], [0011], [0067]).

As to claims 5 and 56:

Malinen expressly teaches:

> wherein each user is authenticated in the telecommunications system by a smart card or subscriber identity module, and in which the authentication storage means respective to that user corresponds to or simulates the smart card for that user ([0024], [0067], [0074], [0080], [0084]).

As to claims 6 and 57:

Malinen expressly teaches:

> wherein the smart card or subscriber identity module authenticates the transaction when the smart card or subscriber identity module is operable in a terminal usable in a mobile and/or cellular telecommunications system (Abstract, [0006], [0009], [0011], [0067], [0074], [0080]).

As to claims 7 and 58:

Malinen expressly teaches:

> wherein the smart card or subscriber identity module is operable to authenticate the terminal in the mobile and/or cellular telecommunications system (Abstract, [0006], [0009], [0011], [0067], [0074], [0080]).

As to claims 11:

Malinen discloses as discussed above; however, *Malinen* does not expressly teach:

> in which the authentication storage means is incorporated on a data carrier for data or software for use by that data processing apparatus.

However, incorporating an authentication storage means on a data carrier is an attribute for the data carrier. Incorporating an authentication storage means on a data carrier is old and well known in the art.

As to claims 12 and 61:

Malinen expressly teaches:

> in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information ([0011], [0062], [0074], [0081], [0085], [0088], Figures 3, 6, 10).

As to claims 36 and 85:

Malinen expressly teaches:

> including routing communications between the authentication storage means and the telecommunications system via the transaction manager ([0009], [0011], [0074]).

As to claims 37 and 86:

Malinen expressly teaches:

wherein the transaction manager is implemented by the data processing apparatus ([0009], [0011], [0074]).

As to claims 38 and 87:

Malinen expressly teaches:

wherein the transaction manager detects the operative coupling of the authentication storage means ([0080]-[0082], [0084]-[0085], Figure 1).

As to claims 39 and 88:

Malinen expressly teaches:

wherein the transaction manager transmits data relating to an authenticated transaction to the entity to which that transaction relates ([0084]-[0086], [0088], [0095]-[0097], [0101]-[0104]).

As to claim 52:

Malinen expressly teaches:

with a data processing apparatus (Abstract, [0005]-[0007], [0070]-[0074]),

a selected one of a plurality of authentication storage means in operative association with the data processing apparatus, each said authentication storage means for storing predetermined authentication information relating to the carrying out of the authentication, the entity being operable to generate transaction data relating to the transaction (Abstract, [0006], [0009], [0011], [0016], [0067]), and

a common telecommunications system which is registerable with the plurality of the authentication storage means ([0157], [0180]),

a communications link with the telecommunications system by which the authentication storage means when operatively associated with the data processing apparatus is operative to carry out the authentication process (Abstract, [0006], [0009], [0011], [0016], [0076], [0079], Figure 8-10), and

authenticating means incorporated in the telecommunications system by which

> the authentication process is carried out and which involves the use of the predetermined authentication information respective to the user stored by the selected one authentication storage means (Abstract, [0006]-[0007], [0009], [0011], [0023], [0070]-[0074]).
>
> the data processing apparatus comprising at least a transaction manager through which communications between the data processing apparatus and the telecommunications system are transmitted and through which the predetermined authentication information is also transmitted between the authentication storage means and the telecommunications system, the transaction manager being implemented by the data processing apparatus (Abstract, [0006], [0009], [0011], [0016], [0076], [0079], Figure 8-10),

Malinen does not expressly teach:

> the predetermined authentication information being stored by each authentication storage means corresponding to information which is used to authenticate a telecommunications terminal of that user in relation to the telecommunications system but the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of that user's telecommunications terminal,

However, Office Notice is taken that *predetermined authentication information stored by each authentication storage means corresponding to information which is used to authenticate a telecommunications terminal of that user in relation to the telecommunications system but the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of that user's telecommunications terminal.* For example, in the related art of user authentication, it is common to employ the use of a portable authentication means. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of *Malinen* with the commonly recognized practice of *predetermined authentication information stored by each authentication storage means corresponding to information which is used to authenticate a telecommunications*

terminal of that user in relation to the telecommunications system but the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of that user's telecommunications terminal.

12. Claims 17, 19-20, 22-23, 25, 27, 66, 68-69, 71-72, 74 and 76 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Malinen* and in view of Tayloe, (US 5,933,785) ("*Tayloe*").

As to claims 17 and 66:

Malinen discloses as discussed above; however, *Malinen* does not expressly teach:

> including operatively coupling the authentication storage means to a carrier.

However, *Tayloe* expressly teaches:

> including operatively coupling the authentication storage means to a carrier (Abstract, Figure 2-3)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify *Malinen* to include the features of *Tayloe* because including a authenticating storage means in a carrier provides protection for it.

As to claims 19 and 68:

Malinen discloses as discussed above; however, *Malinen* does not expressly teach:

> wherein the carrier is operatively coupled to the data processing apparatus by a wireless link.

However, *Tayloe* expressly teaches:

> wherein the carrier is operatively coupled to the data processing apparatus by a wireless link ((Col. 4, lines 45-65)).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify *Malinen* to include the features of *Tayloe* because having a carrier coupled to a apparatus via a wireless link provides for efficient and easy access to processing apparatus.

As to claims 20 and 69:

Malinen discloses as discussed above; however, *Malinen* does not expressly teach:

> wherein the authentication storage means is removably coupled to the carrier.

However, *Tayloe* expressly teaches:

> wherein the authentication storage means is removably coupled to the carrier (Abstract, (Col. 1, lines 14-21), (Col. 2, lines 59-67),(Col. 4, lines 1-17)).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify *Malinen* to include the features of *Tayloe* because it may be desired to interchange authentication storage means with different carriers.

As to claims 22 and 71:

Malinen discloses as discussed above; however, *Malinen* does not expressly teach:

> comprising the step of using said carrier to obtain user security data independently of the data processing apparatus, and analysing the user security data for determining whether to allow access to the predetermined information.

However, *Tayloe* expressly teaches:

> comprising using said carrier to obtain security data independently of the data processing apparatus, and analysing the security data for determining whether to allow access to the predetermined information ((Col. 2, lines 59-67)).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the

invention to modify *Malinen* to include the features of *Tayloe* because it may be desirable to provide some type of security to ensure that only properly authorized user's have access to information on the SIM or smart card.

As to claims 23 and 72:

Malinen discloses as discussed above; however, *Malinen* does not expressly teach:

> wherein the security data is obtained by alphanumeric data entry means.

However, *Tayloe* expressly teaches:

> wherein the security data is obtained by alphanumeric data entry means ((Col. 3, lines 15-22), (Col. 5, lines 55-60), Figure 1).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify *Malinen* to include the features of *Tayloe* because alphanumeric data entry allows for a well know method of inputting data which provides access to control information.

As to claims 25 and 74:

Malinen discloses as discussed above; however, *Malinen* does not expressly teach:

> wherein the user security data comprises a Personal Identification Number (PIN) and the analysing step compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

However, *Tayloe* expressly teaches:

> wherein the user security data comprises a Personal Identification Number (PIN) and the analysing step compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match ((Col. 2, lines 59-67)).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify *Malinen* to include the features of *Tayloe* because it may be desirable to provide some type of security to ensure that only properly authorized user's have access to information on the SIM or smart card.

As to claims 27 and 76:

Malinen expressly teaches:

> wherein communication with the data processing apparatus is controlled by a data processing module (Abstract, [0006]-[0007], [0009], [0011]).

13. Claims 30-34 and 79-83 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Malinen* and in view of *Tayloe* and in further view of Schneier et al., (US 2003/0177347) ("*Schneier*").

As to claims 30 and 79:

The combination of *Malinen/Tayloe* discloses as discussed above; however, the combination of *Malinen/Tayloe* does not expressly disclose:

> wherein the data processing module of the carrier decrypts encrypted data received from the data processing module of the data processing apparatus.

However, *Schneier* expressly teaches:

> wherein the data processing module of the carrier decrypts encrypted data received from the data processing module of the data processing apparatus (See at least [0138]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of *Malinen/Tayloe* to include the features of

Schneier because it may be desirable to maintain data security by ensuring a decryption/encryption process is being employed between device communications with each other.

As to claims 31 and 80:

The combination of *Malinen/Tayloe* discloses as discussed above; however, the combination of *Malinen/Tayloe* does not expressly disclose:

> wherein the data processing module of the carrier encrypts data transmitted to the data processing module of the data processing apparatus.

However, *Schneier* expressly teaches:

> wherein the data processing module of the carrier encrypts data transmitted to the data processing module of the data processing apparatus ([0138]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of *Malinen/Tayloe* to include the features of *Schneier* because it may be desirable to maintain data security by ensuring a decryption/encryption process is being employed between device communications with each other.

As to claims 32 and 81:

The combination of *Malinen/Tayloe* discloses as discussed above; however, the combination of *Malinen/Tayloe* does not expressly disclose:

> wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

However, *Schneier* expressly teaches:

> wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data ([0138]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of *Malinen/Tayloe* to include the features of *Schneier* because it may be desirable to maintain data security by ensuring a decryption/encryption process is being employed between device communications with each other.

As to claims 33 and 82:

The combination of *Malinen/Tayloe* discloses as discussed above; however, the combination of *Malinen/Tayloe* does not expressly disclose:

> wherein the key comprises a shared secret key for each of the respective data processing modules.

However, *Schneier* expressly teaches:

> wherein the key comprises a shared secret key for each of the respective data processing modules ([0212]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of *Malinen/Tayloe* to include the features of *Schneier* because it may be desirable to maintain data security by ensuring a decryption/encryption process is being employed between device communications with each other.

As to claims 34 and 83:

Malinen discloses as discussed above; however, *Malinen* does not expressly disclose:

> wherein the carrier is operatively coupled to a plurality of authentication storage means for respectively enabling the said authentication process and one or more other authentication processes.

However, *Tayloe* expressly teaches:

> wherein the carrier is operatively coupled to a plurality of authentication storage means for respectively enabling the said authentication process and one or more other authentication processes (Abstract, Figure 2-3)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify *Malinen* to include the features of *Tayloe* because including a authenticating storage means in a carrier provides protection for it.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- **Resneck**, (US 2002/0002545); [0026] As shown in FIG. 1, a portable transaction device 10 is conveniently configured to be the size of a credit card that can fit easily into a pocket, a wallet, or a purse. The transaction device 10 has at least one, preferably more than one, storage medium for storing account access information that can be read by a reading device for accessing an anonymous account. For instance, the transaction device 10 includes one or more of a bar code 12, a magnetic strip 14, a CD-ROM 16, a smart-card microprocessor 18 which may be provided with digital storage, and the like. The different storage media on the device 10 may contain the same or different information. The body of the transaction device 10 as shown is a shaped CR-ROM 16. The CD-ROM 16 may be a write-once read-only CD-R. The reading device for reading information stored in the storage media may be an optical scanner, a magnetic data reader, an electronic data reader, or the like. As such, the device 10 may be used in traditional brick-and-mortar establishments as well as in the virtual world of electronic commerce.

- **Rodriquez et al.**, (US 2003/0202661);[0014] In summary, embodiments of the invention provide for the distribution and management of authorization tokens (from a distribution entity 106) that allows a source server (upon successful authentication) to create a working key for encryption of a large video or data file. The process may also insert a small encrypted header in the file that can only be seen by the intended user with the proper authorization token and password. The key is discarded after the encryption process is completed and is never stored. The encrypted file may then travel securely to a destination server. The intended user at the destination server will need a corresponding authorization token (sent by the distribution entity 106) and associated password in order for the software agent on the server to successfully recreate the key for decryption. **The keys are created when the authorization token compares a user password (e.g., in a dongle), and file header for authentication.**

- [0015] During the transport of the video or data file, a second level of encryption may be applied to the file to ensure it is received by authorized recipients only. **Those systems with non-authorized receivers will drop the packets due to wrong authentication (e.g., a smart card may be used for such authentication).**

- [0051] FIGS. 4A and 4B illustrate a secure theater content distribution data flow. Referring to FIG. 4A, a studio/post-production facility (i.e., in a media content provider 102 and protection entity 104) prepares the content 110 for distribution to the distribution entity 106. As illustrated, digital media content 110 such as a movie is obtained from a digital source master 402. Using a studio token, a compression/encryption server 116 prepares (e.g., compresses and encrypts) the content 110. As used herein the studio token 404 may comprise a software code delivered to the studio/post production facility 102/104 (e.g., on a floppy disk). The compression/encryption server 116 authenticates the studio token 404 to determine if the

> studio token 404 received is the studio token 404 expected (i.e., whether the password in the studio token 404 is authentic/valid). In this regard, a variety of authentication techniques may be utilized to authenticate the studio token 404. For example, a dongle may be utilized to authenticate the studio token 404 (as described in more detail below with respect to a theater token). **Further, a password in the dongle may be used to authenticate a user. Alternatively, a stronger authentication mechanism (e.g., biometrics such as fingerprint, or retinal scan readers) may also be used to authenticate the user.**

Any inquiry concerning this communication or earlier communication from the examiner should be directed to Mr. Dante Ravetti whose telephone number is (571) 270-3609. The examiner can normally be reached on Monday – Thursday 9:00am-5:00pm.

If attempts to reach examiner by telephone are unsuccessful, the examiner's supervisor, Mr. Calvin Hewitt may be reached at (571) 272-6709. The fax phone number for the organization where this application or proceeding is assigned is (571) 270-4609.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system see http://pair-direct.uspto.gov. Should you have questions on access to the private PAIR system, please contact the Electronic Business Center (EBC) at 1-(866) 217-9197. If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 1-(800) 786-9199 (IN USA or CANADA) or 1-(571) 272-1000.

/Dante Ravetti/
Examiner, Art Unit 3685
Thursday, February 18, 2010

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685